AF

OK to enter MR

RESPONSE UNDER 37 C.F.R. 1.116 - EXPEDITED PROCEDURE - EXAMINING GROUP 2655

Attorney Docket No. RSW920010010US1/5577-343 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: Hind et al. Conf. No.: 6523
Application No.: 09/765,127 Group Art Unit: 2655
Filed: January 17, 2001 Examiner: Jakieda R. Jackson
For: METHODS, SYSTEMS, AND COMPUTER PROGRAM PRODUCTS FOR SECURELY TRANSFORMING AN AUDIO STREAM TO ENCODED TEXT (amended)

September 9, 2005

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Mailing under 37 CFR § 1.8
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on September 9, 2005.

Carey Gregory

AMENDMENT AFTER FINAL

Sir:

Applicant provides the present response to address the issues raised in the Final Office Action mailed July 12, 2005 ("the Action").

If any extension of time for the accompanying response or submission is required, Applicant requests that this be considered a petition therefor. The Commissioner is hereby authorized to charge any additional fee, which may be required, or credit any refund, to Deposit Account No. 09-0461.

Figure 8 provides a flowchart depicting logic with which a provable chain of evidence may be established for data represented in one or more data streams, according to preferred embodiments of the present invention; and

ok to enter

Figure 9 provides a flowchart depicting logic with which an audio stream may be transformed into notarized text, according to preferred embodiments of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention improves the security of wireless pervasive devices. Central to the invention is a comprehensive, top-down design that focuses first and foremost on security through a security core, as shown at element 150 in Fig. 1. To this secure core, hardware and/or software support for one or more types of personal application functionality can be selectively and dynamically added, resulting in a secure multi-function pervasive device.

The preferred embodiments of the present invention use a multi-processor architecture in which the master processor is a security core 150 which comprises a central processing unit (CPU) 152, a memory 154, and a protected area 156 for storing cryptographic keys. Preferably, a technique such as that defined in commonly-assigned U. S. Patent 09/614982 (serial number 09/614,982) or U. S. Patent 09/614983 (serial number 09/614,983), which are entitled "Methods, Systems and Computer Program Products for Secure Firmware Updates" and "Methods, Systems and Computer Program Products for Rule Based Firmware Updates Utilizing Certificate Extensions", respectively, is used for tightly controlling the code that executes in the security

remains attached to the security core. (Alternatively, an implementation of the present invention may be configured such that this type of firmware revision requires an additional authentication process for the attached component.)

Fig. 2 depicts logic that may be used to implement preferred embodiments of the component authentication process of the present invention. This logic is executed when an application processor is plugged in to the application bus (Block 200). The act of plugging in the processor causes a hardware reset (Block 210) of the application processor (at the electrical level). This hardware reset is preferably initiated as in the prior art, and clears the application processor's memory, sets all hardware components (such as I/O ports, interrupt controllers, timers, and direct memory access controllers) to a known initial state, and causes the application processor's CPU to start executing a predetermined instruction stream at a particular memory location. (This particular memory location is preferably an address within the application processor's ROM, or other on-board memory or storage.) The hardware reset is necessary so that the application processor will be in a known state, so that the security core can vouch for its state thereafter (for the interval over which the application processor remains continuously plugged in to the application bus). Among the initial instructions executed, according to the present invention, will be those required to perform a security handshake (Block 220) between the security core and the application processor. This security handshake is preferably an SSL-like handshake, and its purpose is mutual authentication between the two connecting devices. In preferred embodiments of the present invention, the security handshake is performed using the teachings of commonly-assigned U. S. Patent 09/435,417 (serial number 09/435,417), which is